UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

FARHAD AZIMA, 5921 Ward Parkway Kansas City, Missouri 64113, Plaintiff, v. RAK INVESTMENT AUTHORITY, Sheikh Muhammad Bin Salem Road/E11 Ras al-Khaimah, United Arab Emirates, Defendant.	Civil Action No. 1:16-cv-1948 (KBJ)

FIRST AMENDED COMPLAINT

Plaintiff Farhad Azima ("Plaintiff" or "Mr. Azima"), by and through his undersigned counsel, and pursuant to the Court's Order dated April 25, 2017 (ECF No. 27), files this First Amended Complaint against defendant Ras al Khaimah Investment Authority ("Defendant" or "RAKIA") and alleges as follows:

INTRODUCTION

1. Over the course of approximately one year, RAKIA repeatedly hacked into Mr. Azima's computers and stole his emails and other electronic data. Each instance of hacking constituted an unlawful and actionable accessing of Mr. Azima's computers for which this court has jurisdiction. There were multiple instances of hacking by RAKIA, and at least some of those hackings occurred through U.S.-based IP addresses. RAKIA's hacking went undetected by Mr. Azima as RAKIA amassed documents and data with which it intended to obtain a commercial advantage over Mr. Azima, harm him and his businesses, and threaten him. In furtherance of its

plan, in July 2016, RAKIA – through its lawyer Neil Gerrard, global co-head of Dechert's white collar and securities litigation practice – made such a threat. Just days later, RAKIA made good upon that threat, by creating websites to disparage Mr. Azima and launder his stolen data through portions of the Internet commonly referred to as the Dark Web and by using the stolen emails in an effort to extort millions of dollars from Mr. Azima. Without the disparaging websites, which were created shortly after Mr. Gerrard's threat, it would be nearly impossible to find Mr. Azima's stolen data on the Dark Web, let alone access and download that data.

2. RAKIA is no stranger to hacking. Through its lawyers, its employees, including Jamie Buchanan, and various agents, RAKIA has repeatedly engaged in improper and tortious practices in Ras al Khaimah ("RAK") and elsewhere in order to threaten, extort commercial settlements from, and punish those it deems adversaries to it and RAK. RAKIA's hacking of Mr. Azima is just one of many examples of the improper and tortious conduct that RAKIA has used in connection with its commercial activities.

3. The nature, timing, and sequence of the facts detailed below create an actionable inference and lead to only one reasonable conclusion: that RAKIA was responsible for the hacking of Mr. Azima's computers, the theft of his data, the creation of the websites smearing and commercially disparaging Mr. Azima, and the infliction of commercial harm on Mr. Azima.

4. The hacking of and damage to Mr. Azima's computers, as well as the theft of his data, occurred in the middle of, and in connection with, a commercial engagement by RAKIA of Mr. Azima to perform mediation services. For nearly a year following the hacking, Mr. Azima was unaware that the hacking had occurred or that his data had been stolen. During that time period, he was unaware of anyone possessing or using his data without his permission, including, for example, in any effort to steal his financial information, steal his identity, or threaten him.

RAKIA blamed Mr. Azima for the failed mediation, and RAKIA's counsel threatened Mr. Azima. Within weeks of that threat, websites were created to smear and commercially disparage Mr. Azima. Those websites contained links to BitTorrent sites on the Dark Web that contained Mr. Azima's hacked and stolen data. No one other than RAKIA and Dechert claimed that they had Mr. Azima's stolen data, used the stolen data, or threatened Mr. Azima with his hacked data. To Mr. Azima's knowledge, no one has used the stolen data to access Mr. Azima's financial accounts or steal his identity. In fact, it appears that no one but RAKIA and Dechert have been able to access the vast majority of Mr. Azima's stolen data; even RAKIA's own computer expert could not do so, as documented in a declaration he submitted in this lawsuit. *See* ECF No. 24-1.

5. RAKIA and Dechert have admitted that they have approximately thirty (30) gigabytes (GB) of Mr. Azima's stolen data. Even though the data contain confidential and proprietary business information, and likely include legally privileged communications between Mr. Azima and his counsel, RAKIA and Dechert have refused to return the stolen data despite repeated demands by Mr. Azima. Instead, RAKIA and Dechert have stated that they are free to use Mr. Azima's stolen data as they see fit.

6. Mr. Azima seeks redress of the injuries he has suffered and continues to suffer as the direct and proximate result of RAKIA's hacking and unauthorized access of his computers, theft of his data, and extortionate use of the stolen data against him.

PARTIES

7. Plaintiff Farhad Azima is a U.S. citizen who resides in Kansas City, Missouri. He is a successful businessman who has owned and operated multiple aviation-related companies, including HeavyLift International Airline ("HeavyLift"). Mr. Azima's businesses engage in interstate and foreign commerce.

8. Defendant RAKIA is a commercial investment entity that engages in commercial ventures around the world. On information and belief, RAKIA is headquartered in Ras al-Khaimah, United Arab Emirates ("UAE").

FACTS

Background Regarding Defendant RAKIA

9. The UAE is a federation consisting of seven emirates, one of which is RAK. The UAE government is responsible for developing and ratifying policies, laws, budgets, and agreements governing all of the constituent states, including RAK. Sheikh Saud bin Saqr al Qasimi ("the Ruler"), took over as the ruler of RAK in 2010, and he is a member of the UAE's Federal Supreme Council, which is responsible for overseeing and managing the interests of the UAE and its emirates, including RAK.

10. RAK is one of the poorest emirates within the UAE. RAK has none of the vast oil reserves available in other emirates. Therefore, RAK generates income and wealth, directly or indirectly, through external commercial activities and investments undertaken by and through various entities around the globe.

11. For example, RAK Ceramics is a commercial entity formed for the purpose of creating income and wealth for RAK. As of 2014, RAK Ceramics was the world's largest ceramic tile manufacturer, with a billion dollars in assets, sales of ceramic tiles to more than 135 countries, and branch offices all over the world, including in the United States.

12. RAKIA is also a commercial investment entity that engages in commercial ventures around the world for the purpose of creating income and wealth for RAK. On information and belief, RAKIA is solely and exclusively engaged in commercial activities and does not conduct any political, diplomatic, or other non-commercial functions.

13. RAKIA has the authority to operate both inside and outside RAK, and it has or recently had commercial investments in the Republic of Georgia, India, Armenia, Indonesia, Iran, and other countries. Those investments include ownership of airports, shopping malls, hotels, sea ports, mines, and more.

14. RAKIA frequently files commercial lawsuits arising from its commercial activities, without any allegation or contention that it is somehow immune from litigation. RAKIA has recently filed lawsuits in at least the United Kingdom, Georgia, Switzerland, India, Lebanon, and the UAE. For example, in December 2016, RAKIA commenced a legal proceeding, in the form of an arbitration notice, against the Government of India seeking $44.71 million in damages from the Government of India for allegedly failing to provide bauxite to an aluminum joint venture in India in which RAKIA holds an equity interest. RAKIA has even filed suit against Mr. Azima in the United Kingdom regarding certain commercial activities between RAKIA and Mr. Azima.

15. Moreover, RAK and RAKIA have a long history of threatening those with whom they have business disputes. Those threats are all the more chilling and powerful in a country without due process. Amnesty International has noted widespread due process violations throughout RAK. On information and belief, RAK and RAKIA have abused the legal system in RAK to exert pressure on individuals engaged in business relationships with RAKIA, including, without limitation, by (a) trying individuals in absentia, (b) threatening and imprisoning individuals without trials, (c) holding those with whom RAK and RAKIA have disputes in a dungeon located in the Ruler's Palace, and (d) prohibiting individuals from leaving the UAE until they paid money to resolve claims made by RAKIA. On further information and belief, RAKIA has also obtained INTERPOL red notices against individuals with whom it has had

commercial disputes. Often RAK defies UAE law in the ways in conducts its business. Mr. Azima has had nothing but cordial relationships with the other emirates and the UAE and holds them in high regard.

16. RAK and RAKIA have also engaged in commercial espionage and spying by, among other things, engaging in computer data hacking of its business partners and adversaries. It has been widely and extensively reported that the UAE, by and through its constituent members, including RAK, has repeatedly engaged in state-sponsored hacking of adversaries by, among other things, surreptitiously installing spyware in order to monitor and steal communications, just as happened to Mr. Azima. The hacking program has been documented from at least 2012 and reportedly has involved its use of sophisticated hacking software and experts. According to an article in *The New York Times*, through 2015, the UAE spent hundreds of thousands of dollars to hack more than 1,000 people.

17. It has been reported that the UAE contracted with at least three different companies to purchase hacking software. For example, between 2012 and 2016, CyberPoint provided software that used Twitter, spear-phishing emails, and a malicious URL shortening service to entice targets to click on links that would then infect their computers with dangerous spyware. As alleged herein, the hacking of Mr. Azima by RAKIA fits, and is fully consistent with, the pattern and practice of commercial espionage and hacking in which emirates of the UAE, including RAK, have reportedly been regularly engaged.

Mr. Azima's Commercial Relationship with RAK and RAKIA

18. RAKIA and Mr. Azima have an extensive history of commercial dealings, including multiple business ventures that they engaged in together and multiple requests by RAKIA for Mr. Azima to help it mediate business disputes. Indeed, over the course of their

commercial relationship, RAKIA has paid Mr. Azima more than $7 million, all in relation to commercial activity.

19. In April 2007, RAK, RAKIA, and Mr. Azima created a joint venture, RAK-HeavyLift Training Academy, jointly owned by Mr. Azima's company, HeavyLift, and RAK Airways. RAKIA guaranteed RAK Airways' performance under the joint venture agreement. The joint venture was formed to build a flight training academy in RAK and train pilots. Mr. Azima was a director of the joint venture.

20. Additionally, in November 2009, RAK purchased 51 percent of Mr. Azima's company, HeavyLift, for $3.8 million. RAKIA consented to the share purchase agreement. Throughout the commercial relationship between Mr. Azima and RAK in the joint-ownership of HeavyLift, RAK wired funds in U.S. dollars to the U.S. bank accounts of Mr. Azima or HeavyLift.

21. Mr. Azima and RAKIA repeatedly explored other business opportunities. For example:

- In 2007-2008, RAK hired Mr. Azima to resolve a dispute between RAK and Boeing regarding the acquisition of a new Boeing 737 aircraft.
- In 2008-2009, RAKIA requested Mr. Azima's assistance regarding a dispute relating to the America's Cup sailboat race, which was supposed to take place off the coast of RAK.
- Mr. Azima and RAKIA discussed at length the development of an aviation maintenance facility in RAK, a housing and hotel business in Iraq and Kurdistan, and a steel construction business.

- In the fall of 2015, Mr. Azima and RAKIA engaged in preliminary discussions regarding an Intelligence, Surveillance, and Reconnaissance (ISR) joint venture between RAKIA and JFJ International Logistics, a company in which Mr. Azima owned an interest.
- In the summer of 2016, Mr. Azima and RAKIA, through its representative Jamie Buchanan, discussed RAKIA and Mr. Azima investing in a munitions factory.

22. To facilitate the Ruler's ability to conduct commercial activities around the globe, including through RAKIA, the Ruler asked Mr. Azima, from time to time, to introduce him to global business leaders and multiple heads of state. The Ruler was Mr. Azima's guest at events with world leaders, and Mr. Azima introduced the Ruler to people who could help raise RAK's global profile and increase RAK's and RAKIA's business potential. For example, Mr. Azima hosted the Ruler and his daughter at the annual meeting of President Bill Clinton's Clinton Global Initiative ("CGI") in New York City in 2011. Mr. Azima arranged for the Ruler to become a CGI member and facilitated numerous introductions through the CGI and other international organizations in the United States.

Mr. Azima's Mediation of RAKIA's Dispute with Khater Massaad

23. Consistent with the long-standing business and commercial relationship between RAK, RAKIA, and Mr. Azima, in the Fall of 2015, RAKIA asked Mr. Azima to mediate a dispute between RAKIA and its former CEO, Dr. Massaad, among others. Mr. Azima agreed to provide such mediation services, and, over the course of several months, met numerous times with RAKIA's representative Jamie Buchanan and RAKIA's counsel, Neil Gerrard of Dechert LLP. Mr. Azima spent significant time and incurred significant expenses serving as the mediator

for that matter with the expectation that he would be compensated for his services and expenses. His services were terminated by RAKIA, and RAKIA failed to compensate him for his time or expenses.

24. In the Fall of 2015, during the mediation, Mr. Azima frequently communicated with Mr. Buchanan and Mr. Gerrard, through emails and phone calls from and to Mr. Azima in the United States, as well as through multiple meetings, some of which took place in the United States. On September 23, 2015, Mr. Buchanan and Mr. Gerrard met with Mr. Azima in New York to discuss the possible terms of a global settlement between RAKIA and Dr. Massaad.

25. On October 14, 2015, the Ruler emailed Dr. Massaad expressing the Ruler's supposed disappointment regarding unspecified "findings" by Dechert and its experts relating to certain alleged actions by Dr. Massaad. That same day, and as detailed below, Mr. Azima's computers were surreptitiously hacked.

The Hacking of Mr. Azima's Computers

26. On or about October 14, 2015, Mr. Azima's computers were improperly and surreptitiously accessed from two U.S.-based IP addresses, one in Florida and one in New York. An IP address is a unique identifier given to a computer connected to the internet that provides information about the location of that computer.

27. In the days leading up to the hack, without his knowledge, Mr. Azima's computer received multiple spear-phishing emails. Spear-phishing is a sophisticated form of hacking in which the hacker sends fake correspondence that is designed to look like something the target would normally receive with the intention of collecting confidential information or receiving improper access to computers and accounts. In contrast to phishing, spear-phishing is directed at

a specific target with correspondence that is designed to entice that target to open the email or message.

28. At least two of the emails contained information relating to RAKIA and the UAE. At least one of the spear-phishing emails Mr. Azima's computer received on or about October 14, 2015 included allegations similar to allegations that RAKIA has made against Mr. Azima in the past. At least one of the spear-phishing emails Mr. Azima received on or about October 14, 2015 included what appeared to be a link to a video about an aircraft from the UAE. Both of these emails contained malicious links.

29. The hackers obtained unlimited access to Mr. Azima's computers until Mr. Azima learned of the hacking in August 2016, after which he changed his passwords and increased his security measures.

30. Because the hackers had unlimited access to Mr. Azima's computer and his email accounts, the hackers were able to steal his data, monitor his communications in real time, send emails that appeared to come from Mr. Azima, and delete valuable data from Mr. Azima's computers.

31. Before August 2016, Mr. Azima did not know that his computers had been hacked and that the hackers were able to monitor his communications. Accordingly, prior to learning of the hacking, Mr. Azima continued to communicate with RAK's representatives, Mr. Buchanan and Mr. Gerrard, as well as Dr. Massaad, regarding the mediation. During this time period, Mr. Azima also met with Mr. Buchanan and Mr. Gerrard multiple times, including in New York in February 2016, and he engaged in extensive communications with his attorneys regarding privileged matters, some of which related to his commercial interactions with RAKIA.

32. RAKIA's counsel has stated that, prior to September 2016, RAKIA engaged experts to search for information regarding Mr. Azima and that those searches included searches for stolen information. RAKIA's counsel has claimed that those searches in fact yielded Mr. Azima's stolen data, including from BitTorrent sites on the Dark Web. RAKIA's counsel has admitted that RAKIA and Dechert are presently in possession of 30 GB of Mr. Azima's stolen data. As of the filing of this First Amended Complaint, RAKIA and RAKIA's counsel are the only persons or entities known to Mr. Azima to have his stolen data.

33. As a result of the actions of RAKIA and its agents, Mr. Azima's aggregate losses far exceed $5,000 during a one-year period. Mr. Azima hired computer experts to take responsive measures regarding the hacking and the theft of Mr. Azima's data. The experts determined that Mr. Azima's computers had been damaged by the hacking and identified malware on his computers, requiring the replacement of Mr. Azima's infected computers. This caused a disruption in his businesses. Mr. Azima has been unable to restore all of his data that he had prior to the hacking.

The Disparagement of Mr. Azima and the Laundering of His Data Through BitTorrent Sites

34. Mr. Azima served as mediator in the RAKIA-Massaad matter until the end of July 2016. In July 2016, it appeared that the parties had reached a tentative settlement. However, RAKIA and its counsel suddenly and inexplicably reversed course and refused to finalize the settlement. They blamed Mr. Azima for the lack of a settlement between RAKIA and Dr. Massaad.

35. After several intense discussions between Mr. Azima and RAKIA's representative and counsel, on or about July 23, 2016, RAKIA's counsel, Neil Gerrard of Dechert LLP, threatened Mr. Azima that RAKIA and he would make Mr. Azima "collateral damage" in the

war RAKIA intended to wage against its former chief executive officer, Dr. Massaad. When Mr. Azima asked Mr. Gerrard if Mr. Gerrard's statement was a threat, Mr. Gerrard said it was not just a threat because Mr. Gerrard delivered on his promises. Mr. Buchanan and Mr. Gerrard refused Mr. Azima's request for copies of the handwritten notes that Mr. Gerrard's colleague at Dechert took during the July 2016 meeting in which Mr. Gerrard threatened Mr. Azima.

36. Within a week of Mr. Gerrard's threat, RAKIA commenced a prolonged negative public relations campaign against Dr. Massaad and Mr. Azima that was obviously intended to disparage Dr. Massaad and Mr. Azima.

37. For example, Mr. Azima subsequently learned that, on or about July 29, 2016, the website www.khater-massaad.com was created to disseminate negative information about Dr. Massaad and to parrot the claims that RAKIA made against Dr. Massaad during the mediation.

38. Shortly thereafter, two other websites containing similar, unsubstantiated and negative allegations about Mr. Azima were created. These websites also included claims that RAKIA had previously made against Mr. Azima. The very first post on one of those websites was made from the UAE, of which RAK is a constituent member.

39. The websites relating to Mr. Azima included links to BitTorrent sites that included Mr. Azima's hacked files. One of those BitTorrent sites included a portion of Mr. Azima's iCloud backup data, which included iMessages, SMS messages, Viber messages, WhatsApp messages, videos, contact details, call history, calendar, appointment history, voice messages, recordings, and photos from Mr. Azima's computers. Several computer experts, including an expert whom RAKIA retained to submit a declaration to this Court (*see* ECF No. 24-1), have been unable to access another BitTorrent site, containing the vast majority of Mr.

Azima's data. This unavailable BitTorrent site allegedly contains roughly 25 GB of Mr. Azima's 30 GB of stolen data, including privileged and confidential communications.

The "Availability" of Mr. Azima's Stolen Data

40. BitTorrent index sites provide a platform to download stolen files shared over the BitTorrent protocol ("BitTorrent sites"). BitTorrent sites are sometimes referred to as being part of the "Dark Web" as their content is not available to and downloadable by the general public without specialized software and expertise. First, without links to the BitTorrent sites, it is extremely difficult to find specific data housed on BitTorrent sites. In this case, on information and belief, RAKIA and/or its agents created the only websites that link to Mr. Azima's data. Second, even after a user locates the relevant data, it is not possible to download the data from the BitTorrent sites unless a complete copy of the data is available. No one except RAKIA and Dechert is known to have been able to access a complete copy of Mr. Azima's stolen data from the BitTorrent sites. Lastly, because BitTorrent is known to include substantial malware, the sites are often blocked by cyber-security software.

41. In order to gain the ability to download data from BitTorrent sites, a user must have specific indexing information as well specialized software and expertise. Accordingly, there is no way for a typical user to find content without links or websites pointing the user to the relevant data. On information and belief, in order to create the manufactured pathways necessary to locate the data, RAKIA and/or its agents created the websites disparaging Mr. Azima and providing links to BitTorrent sites that allegedly housed Mr. Azima's stolen data.

42. Without those websites, which were created shortly after Mr. Gerrard's threat against Mr. Azima, it would be nearly impossible to find Mr. Azima's stolen data on the BitTorrent sites, let alone access and download that data.

43. Even after the websites were created, it has not been possible to access Mr. Azima's data. As RAKIA's expert declared to this Court, in order to download from BitTorrent sites, a complete copy of the data needs to be available. RAKIA's expert was not able to independently access the vast majority of the stolen data that RAKIA possesses.

44. It is widely known that BitTorrent sites often contain stolen files, such as pirated movies and other misappropriated data. It is also commonly known that the micro-sites associated with BitTorrent sites contain substantial malware and software viruses which could infect the computers and systems of anyone who accesses those sites.

45. BitTorrent sites are often used to download misappropriated files because the BitTorrent platform inhibits the identification of its users. As a result, BitTorrent sites can be used to "launder" data and obscure the origin of the data. BitTorrent sites can also make downloading large files more efficient in certain circumstances, but only where the files being downloaded are popular, such as music and movies, and are possessed by many users.

46. Stolen and misappropriated data is disaggregated across BitTorrent sites and related micro-sites, which makes it highly unlikely, if not impossible, for a legitimate business to know independently, and without involvement in the misappropriation or direction, that such data exist on websites or how to access such data. In other words, the average computer user would have to be "tipped off" that the data is hidden on a BitTorrent site or related micro-sites and would need specific information and undertake special measures to navigate the websites in order to access the data on those websites.

47. Any legitimate business that received notice and direction from a third-party regarding the existence of certain data on BitTorrent sites and related micro-sites would or should know that such data had been misappropriated or stolen.

48. There is no normal or proper reason for a legitimate business to access BitTorrent sites or related micro-sites. In fact, most security software employed by legitimate businesses is designed to completely block users from accessing any BitTorrent sites or related micro-sites due to the security risk those sites pose.

RAKIA's Extortive Use of the Hacked and Stolen Data

49. On September 23, 2016, Mr. Azima's counsel in Washington, D.C., received a demand letter via email from Mr. Gerrard's partner, David Hughes of Dechert, LLP, attaching exhibits. The purpose of the letter was to make an extortionate demand on Mr. Azima. In the letter, Dechert demanded that Mr. Azima pay RAKIA and an affiliate of RAKIA $4,162,500 U.S. dollars in a bank account titled "Dechert LLP USD Client A/c," or else RAKIA would sue Mr. Azima. Dechert claimed that this demand was based upon information that RAKIA had "recently obtained . . . via publically available internet sources," *i.e.*, Mr. Azima's stolen data.

50. Dechert attached to the letter copies of some of Mr. Azima's stolen files. The documents contain proprietary and confidential information, including protected pricing information relating to Mr. Azima's businesses.

51. As an additional threat, and further linking this action to the United States, including potentially U.S. agencies and officials located in Washington, D.C., Dechert stated in the September 23, 2016, letter that RAKIA "currently intends to seek advice from its US lawyers as to the possibility of raising its concerns about [Mr. Azima's alleged conduct] with the relevant US enforcement agency." This additional threat is or would be a violation of Rule 8.4(g) of the District of Columbia Bar's Rules of Professional Conduct, which deems it "professional misconduct" for an attorney to "[s]eek or threaten to seek criminal charges . . . solely to obtain an advantage in a civil matter." It is evident that, by making this threat, Defendant's counsel intended to extort Mr. Azima to transfer $4,162,500 to the bank account titled "Dechert LLP

USD Client A/c" on or before September 30, 2016. RAKIA claims to have made good on its threat to report bogus allegations to officials of the United States Government, including officials in Washington, D.C., for the purpose of inflicting further financial, reputational, and legal harm on Mr. Azima. The use of illegally and improperly obtained data by RAKIA and Dechert under such circumstances is tortious and improper.

52. Mr. Azima's counsel subsequently received an additional copy of Defendant's counsel's September 23, 2016, demand and threat letter by an overnight service, delivered to Mr. Azima's counsel in Washington, D.C.

53. On September 28, 2016, Mr. Azima's counsel asked Defendant's counsel to identify "the website(s) from which some of the materials you attach are located." In an email to Mr. Azima's counsel, on September 29, 2016, Mr. Hughes wrote that the "[d]ocuments were obtained from a number of sites" including multiple torrent sites. Hughes explained that he had been "advised [by some person] that these sites may contain viruses and should only be accessed with professional assistance." Mr. Hughes made no mention of the websites disparaging Mr. Azima that were created shortly after Mr. Gerrard's threat against Mr. Azima.

54. From the hacking of Mr. Azima's computers in or about October 2015 until the filing of this First Amended Complaint, no person or entity other than RAKIA or Dechert is known to have Mr. Azima's stolen data, and no person or entity used the hacked data to steal Mr. Azima's identity or financial information. No fraud regarding the bank accounts used by Mr. Azima, his businesses, or associates, has occurred.

RAKIA and Dechert Have Admitted to Having and Using the Data

55. Mr. Azima's counsel immediately informed Dechert that the stolen data likely contained privileged material and demanded that all privileged communications be returned to

Mr. Azima and not reviewed. RAKIA and Dechert have refused to return any of Mr. Azima's stolen data, including the privileged material.

56. RAKIA and Dechert have claimed that they are free to use Mr. Azima's stolen data "as they see fit."

57. In correspondence between Mr. Azima's counsel and RAKIA's counsel, RAKIA and Dechert have admitted the following:

- RAKIA engaged experts to monitor Mr. Azima;
- Dechert is in possession of 30 GB of Mr. Azima's stolen data;
- Dechert was given all of that data by RAKIA;
- RAKIA and/or its agents downloaded Mr. Azima's data;
- RAKIA's experts searched sites known to contain hacked data;
- Dechert has and continues to review Mr. Azima's stolen data;
- Separate from the stolen documents, Dechert has tens of thousands of documents on its servers related to Mr. Azima;
- The stolen data of Mr. Azima that Dechert possesses may contain privileged information;
- Dechert refuses to return Mr. Azima's stolen data, including privileged material, to him or tell Mr. Azima what data of his they possess; and
- Dechert and RAKIA contend that they are free to use Mr. Azima's data however they "see fit."

58. A computer expert retained by RAKIA to submit a declaration to this Court admits that he was unable to download the vast majority of Mr. Azima's stolen data that RAKIA claims is publicly available.

59. Therefore, no known person or entity, other than RAKIA and Dechert, has been able to access, download, or possess the vast majority of Mr. Azima's stolen data other than RAKIA and Dechert.

60. From and based on the foregoing facts, the only possible inference and reasonable conclusion is that RAKIA and its agents are responsible for the hacking of Mr. Azima's computers, the theft of his data, the posting of the stolen data to BitTorrent sites, and the creation of the websites smearing Mr. Azima. The hacking of Mr. Azima's computers occurred in the middle of, in connection with, as a result of, and was motivated by a commercial engagement by RAKIA of Mr. Azima. For nearly a year following the hacking, no person or entity used the data against Mr. Azima to steal his financial information, steal his identity, or threaten him. Then, as the discussions that Mr. Azima was engaged by RAKIA to mediate broke down, RAKIA blamed Mr. Azima, and RAKIA's counsel threatened to make Mr. Azima "collateral damage." Within weeks of that threat, websites were created to disparage and smear Mr. Azima. Those websites contained links to BitTorrent sites that purported to contain Mr. Azima's hacked and stolen data. No person or entity other than RAKIA and Dechert has attempted to use the stolen data against Mr. Azima. Though RAKIA is in possession of 30 GB of Mr. Azima's stolen data and has attempted to use it to extort Mr. Azima, the vast majority of Mr. Azima's stolen data remains inaccessible to everyone but RAKIA and Dechert (including even RAKIA's own expert).

JURIDICTION AND VENUE

61. This Court has subject matter jurisdiction over this case pursuant to 28 U.S.C. § 1332(a)(2) because, on information and belief, RAKIA was formed under the laws of a foreign state. To the extent RAKIA is deemed an instrumentality of a foreign state within the meaning of 28 U.S.C. § 1603(b) of the Foreign Sovereign Immunities Act ("FSIA"), this Court has

subject matter jurisdiction over this case pursuant to 28 U.S.C. § 1330(a) because, even if RAKIA is ultimately determined to be an instrumentality of a foreign state within the meaning of 28 U.S.C. § 1603(a), RAKIA is not entitled to immunity under the FSIA pursuant to the exceptions set forth in 28 U.S.C. § 1605(a)(2) and § 1605(a)(5). Under such circumstances, this court has supplemental jurisdiction over the asserted common law counts under 28 U.S.C. § 1367.

62. Venue properly lies in this Court pursuant to 28 U.S.C. § 1391(b)(2) and 28 U.S.C. § 1391(b)(3) because a substantial part of the events or omissions giving rise to some or all of Plaintiff's claims occurred in this district and/or Defendant is subject to the Court's personal jurisdiction with respect to this case. Pursuant to Fed. R. Civ. P. 12, Defendant has waived any objection to venue in this Court except to the extent it relies upon the doctrine of *forum non conveniens*.

Pursuant to 28 U.S.C. § 1605(a)(2), RAKIA is not entitled to immunity

63. As discussed above, at the time of the hacking of his computers, Mr. Azima was engaged in both a regular course of commercial activity with RAKIA and a particular commercial transaction, namely serving as a mediator for RAKIA's dispute with Dr. Massaad.

64. Mr. Azima's regular course of commercial activity included, but was not limited to, the creation of a joint venture between RAK Airways and Mr. Azima's company HeavyLift, guaranteed by RAKIA, to create a flight training academy in RAK; RAK Trans Holding acquiring a controlling interest in HeavyLift with RAKIA consenting to the agreement; Mr. Azima's assistance in resolving a dispute between RAK and Boeing; negotiations between Mr. Azima and RAKIA regarding the development of an aviation maintenance facility in RAK, a housing and hotel business in Iraq and Kurdistan, and a steel construction and fabrication business; assisting with the sale of RAKIA's assets in Georgia, including the Sheraton hotel in

Tbilisi; preliminary discussions regarding the possibility of an ISR joint venture between RAKIA and JFJ International Logistics, and Mr. Azima's role as a mediator for RAKIA in the dispute with Dr. Massaad. The actions of RAKIA and its agents, as alleged herein, were intended and designed to cause and inflict harm and damage upon Mr. Azima because of, related to and in connection with the commercial activities between Mr. Azima and RAKIA. In its September 23, 2016 letter to Mr. Azima's counsel, Dechert specifically identified multiple commercial relationships in which RAKIA and Mr. Azima were engaged and to which the hacking was connected.

65. This action is based on and arises from the hacking and unauthorized access of Mr. Azima's computers, the theft of Mr. Azima's data, the commercial disparagement of Mr. Azima, and the extortive use of the data by RAKIA and Dechert against Mr. Azima in connection with and in order to gain an advantage in RAKIA's commercial relationship with Mr. Azima.

66. Specifically, the hacking, theft, and extortive use of Mr. Azima's data by RAKIA and its agents were explicitly connected to RAKIA's commercial agreement to have Mr. Azima serve as a mediator for RAKIA. RAKIA engaged the services of Mr. Azima as a mediator, not as an employee of the RAK government. That relationship constituted commercial activity of RAKIA, and RAKIA's actions were taken in connection with that activity.

67. Mr. Azima was engaged as a mediator by RAKIA at the time of the hacking of his computers in October 2015. The hack was designed by RAKIA to gain leverage and coercive influence over Mr. Azima. When the settlement discussions between RAKIA and Dr. Massaad broke down, RAKIA and Dechert blamed Mr. Azima for the lack of a settlement. At a meeting in July 2016, frustrated with the state of the negotiations, RAKIA's counsel, Mr. Gerrard,

threatened Mr. Azima. Shortly after that meeting, websites were created by RAKIA and its agents to disparage and smear Mr. Azima, and most importantly to make public the data on the BitTorrent sites. Those websites contained links to BitTorrent sites, at least one of which contained Mr. Azima's stolen data.

68. RAKIA, directly and through its agents, took the acts alleged herein in order to gain an advantage over Mr. Azima in his commercial dealings with RAKIA and to inflict commercial and financial harm on Mr. Azima.

69. Because the unauthorized access, theft, and extortive use of Mr. Azima's data by RAKIA and its agents occurred, and caused direct effects, in the United States in connection with the commercial activity of RAKIA, RAKIA is not immune from suit. In addition, even if none of the alleged acts occurred in the United States, RAKIA would not be immune from suit because the acts were in connection with the commercial activity of RAKIA and caused a direct effect in the United States.

70. Furthermore, RAKIA has waived, and is foreclosed from asserting, any immunity by engaging in serial litigation throughout the world, including litigation against Mr. Azima regarding certain of their commercial activities.

71. As a result of these actions, Mr. Azima suffered losses and damages in the United States, including those resulting from the unlawful accessing of his computers, the theft of his data, loss of his computers, and the disruption of his business.

Pursuant to 28 U.S.C. § 1605(a)(5), RAKIA is not entitled to immunity

72. Even if RAKIA were not exempt from immunity under 28 U.S.C. § 1605(a)(2), this Court would still have jurisdiction over RAKIA under § 1605(a)(5).

73. This action is premised upon money damages sought against RAKIA for damage to and loss of property occurring in the United States and caused by the tortious acts of RAKIA

and its agents, including, without limitation, the unlawful hacking and unauthorized access of Mr. Azima's computers and the unlawful theft of Mr. Azima's data.

74. As discussed above, on and after October 14, 2015, Mr. Azima's computers were repeatedly hacked in anticipation of using the data against Mr. Azima. On information and belief, the hackers infiltrated Mr. Azima's computers numerous times over the course of a year, and at least some of those hackings occurred from IP addresses in Florida and New York.

75. This unauthorized access resulted in damage to Mr. Azima's computers, the unlawful accessing of his computers, the unlawful theft of his data, and the disruption of Mr. Azima's business and the destruction of his computers in the United States.

76. Because the unauthorized access occurred in the United States and the damage to Mr. Azima's businesses occurred in the United States, RAKIA is not entitled to immunity under 28 U.S.C. § 1605(a)(5), even if it is not exempt under § 1605(a)(2).

COUNT I
(Violation of Computer Fraud And Abuse Act; Aiding and Abetting Violation of the Computer Fraud And Abuse Act)
(18 U.S.C. § 1030, et seq.)

77. Plaintiff incorporates by reference, as if fully set forth herein, the allegations contained in paragraphs 1-76, above.

78. Mr. Azima's computers are protected computers as defined by the CFAA because they are used in and affect interstate commerce, foreign commerce, and communication. Mr. Azima's businesses are national and international businesses. His computers were and are used to engage in national and international communications and transactions. RAKIA's hack of Mr. Azima's computers included not only a hack of his U.S.-based business and personal laptops, but also a hack of his business and personal email accounts and his iCloud data.

79. RAKIA, directly and/or through its agents, knowingly and intentionally accessed, or knowingly and intentionally aided and abetted a person or persons to access, Mr. Azima's computers without authorization and thereby obtained, by its own admission, approximately 30 GB of data from Mr. Azima's computers in violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(2).

80. Additionally, RAKIA, directly and/or through its agents, knowingly and intentionally accessed, or knowingly and intentionally aided and abetted a person or persons to access, Mr. Azima's computers without authorization and as a result, recklessly caused damage to his computer, as described below, in violation of 18 U.S.C. § 1030(a)(5)(B).

81. In addition, RAKIA, directly and/or through its agents, knowingly and intentionally accessed, or knowingly and intentionally aided and abetted a person or persons to access, Mr. Azima's computers without authorization and as a result, caused damage to Mr. Azima's computers and an actionable loss to Mr. Azima, as described below, in violation of 18 U.S.C. § 1030(a)(5)(C).

82. Mr. Azima suffered damage to his computers and his businesses as defined in 18 U.S.C. § 1030(e)(8) because he has suffered impairment to the integrity and availability of his data and his computers. On information and belief, as a result of the hacking of his computers, some of Mr. Azima's data has been deleted. In addition, Mr. Azima had to dispose of and replace computers that were infected as part of the hacking. Lastly, Mr. Azima's businesses experienced a disruption in service after he learned of the hacking and took steps to address the breach and unlawful accessing of his computers.

83. Mr. Azima also suffered loss as defined in 18 U.S.C. § 1030(e)(11) because he incurred reasonable costs associated with responding to the hacking, conducting a damage assessment, and attempting to restore his data and computers.

84. As a result of RAKIA's actions, Mr. Azima has incurred aggregate losses far in excess of $5,000 during a one-year period.

85. The actions of RAKIA have directly and proximately caused Mr. Azima to suffer substantial injury and legally cognizable damages in an amount to be determined at trial.

86. In addition, as a result of the past and continuing violations, Mr. Azima has suffered, and will likely continue to suffer, certain irreparable harm to his person, reputation and business.

COUNT II
(Conversion; Aiding and Abetting Conversion)

87. Plaintiff incorporates by reference, as if fully set forth herein, the allegations contained in paragraphs 1-86, above.

88. RAKIA, directly and/or through its agents, knowingly and intentionally hacked, misappropriated, stole and/or improperly came into possession of, or knowingly and intentionally aided and abetted a person or person to hack, misappropriate, steal and/or improperly come into possession of, the internal and confidential electronic data of Mr. Azima. RAKIA has exercised wrongful dominion and control over that data in violation of Mr. Azima's rights.

89. The data that RAKIA stole, misappropriated, or improperly came into possession of included proprietary business information with substantial commercial value, such as protected pricing information and other confidential documents relevant to commercial dealings

with both RAKIA and others. That data also included privileged communications between Mr. Azima and his attorneys relating to matters that involved RAKIA, as well as other matters.

90. As a result of RAKIA's tortious actions, some of Mr. Azima's data have been stolen and/or deleted from his computers and have not been returned or restored.

91. Mr. Azima has repeatedly requested that RAKIA and its counsel return his stolen data, including his privileged correspondence, but RAKIA and its counsel have consistently refused to return the stolen data.

92. The tortious actions of RAKIA alleged herein, including, without limitation, the deletion of Mr. Azima's data and refusal to return Mr. Azima's stolen data, constitute the unlawful conversion of Mr. Azima's property.

93. RAKIA's tortious actions were taken and motivated by animus, ill-will and malice towards Mr. Azima and with the specific intent of harming Mr. Azima in his person and his business.

94. The tortious actions of RAKIA have directly and proximately caused Mr. Azima to suffer substantial injury and legally cognizable damages in an amount to be determined at trial, including but not limited to the deletion, theft and unlawful withholding of Mr. Azima's data.

95. In addition, as a result of the past and continuing tortious conduct by RAKIA, Mr. Azima has suffered, and will likely continue to suffer, certain irreparable harm to his person, reputation and business.

COUNT III
(Unfair Competition)

96. Plaintiff incorporates by reference, as if fully set forth herein, the allegations contained in paragraphs 1-95, above.

97. RAKIA, directly and/or through its agents, knowingly and intentionally engaged in improper and illegal conduct against Mr. Azima in order to gain an unfair advantage in business competition and commercial activities with Mr. Azima.

98. The tortious, wrongful and improper actions of RAKIA and/or its agents included, without limitation, commercial disparagement of Mr. Azima, the interference with his business computers, the theft of Mr. Azima's data and the use of threats and extortion in order to cause Mr. Azima to pay substantial amounts of money to RAKIA and/or its agents, particularly through threats of baseless lawsuits.

99. The tortious actions of RAKIA were taken and motivated by animus, ill-will and malice towards Mr. Azima and with the specific intent of harming Mr. Azima in his person and his business.

100. The tortious actions of RAKIA included, without limitation, representations that RAKIA knew were false or were made with reckless disregard as to their falsity. These representations were designed to deceive and mislead potential business associates of Mr. Azima.

101. The tortious actions of RAKIA and/or its agents could not have been motivated by any legitimate business rationale.

102. The tortious actions of RAKIA and/or its agents have directly and proximately caused Mr. Azima to suffer substantial injury and legally cognizable damages in an amount to be determined at trial.

103. In addition, as a result of the past and continuing tortious conduct by RAKIA, Mr. Azima has suffered, and will likely continue to suffer, certain irreparable harm to his person, reputation and business.

PRAYER FOR RELIEF

On the basis of the foregoing, and such evidence as Plaintiff will present at trial, Plaintiff Farhad Azima requests the entry of judgment in his favor and against Defendant RAK Investment Authority ("RAKIA") on all counts of the First Amended Complaint and the award of the following relief:

104. All statutory and compensatory damages incurred by Plaintiff as a result of the violations of 18 U.S.C. § 1030, et seq., as alleged above, in an amount to be determined at trial.

105. Compensatory damages incurred by Plaintiff as a result of the actions of Defendant and its agents, in an amount to be determined at trial.

106. Punitive damages in an amount not less than Twenty Million Dollars ($20,000,000.00).

107. A mandatory injunction requiring Defendant and its agents to return to Plaintiff all electronic data and other property of Plaintiff that are in the possession, custody, or control of Defendant and its agents, including all copies thereof.

108. A prohibitory injunction obligating Defendant and its agent to refrain in the future from accessing Plaintiff's computers and/or misappropriating or otherwise accessing Plaintiff's internal and confidential electronic data or other property.

109. Pre-judgment and post-judgment interest in the amounts and at the rates provided by law.

110. The costs and expenses, including reasonable attorney's fees, incurred by Plaintiff in this action and as a result of the actions of Defendant and its agents alleged herein.

111. Such other and further relief as the Court deems just and proper.

Dated: May 16, 2017

Respectfully submitted,

/s/ Kirby D. Behre

Kirby D. Behre (D.C. Bar # 398461)
Timothy O'Toole (D.C. Bar # 469800)
Charles F. B. McAleer Jr. (D.C. Bar # 388681)
Ian A. Herbert (D.C.Bar # 1019902)
Miller & Chevalier Chartered
900 16th Street, NW
Washington, D.C. 20006
Tel: (202) 626-5800
Fax: (202) 626-5801
Email: kbehre@milchev.com
Email: totoole@milchev.com
Email: cmcaleer@milchev.com
Email: iherbert@milchev.com

JURY DEMAND

Plaintiff Farhad Azima respectfully requests a trial by jury of all issues so triable.

/s/Kirby D. Behre
Kirby D. Behre

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that, on this 16th day of May, 2017, a true and genuine copy of the foregoing was sent by ECF to the following:

Linda C. Goldstein (*pro hac vice*)
Dechert LLP
1095 Avenue of the Americas
New York, NY 10036
Telephone: (212) 698-3500
Linda.goldstein@dechert.com

D. Brett Kohlhofer (D.C. Bar # 1022963)
Dechert LLP
1900 K Street, NW
Washington, D.C. 20006
Telephone: (202)261-3349
d.brett.kohlhofer@dechert.com

Attorneys for Defendant

/s/Kirby D. Behre
Kirby D. Behre